APPLIED POSTQUANTUM CRYPTOGRAPHY FOR IOT

Lucie Popelová
Bachelor Degree Programme (3), FEEC BUT
E-mail: xppopel04@vutbr.cz

Supervised by: Lukáš Malina
E-mail: malina@feec.vutbr.cz

Abstract: In the last decades there has been such a fundamental development in the technologies including postquantum technologies. It is necessary to focus on postquantum cryptography which is able to resist quantum attacks and secure our systems. This work deals with postquantum protocols that are analysed and measured on the IoT device. Our experimental results are used to find the most effective postquantum protocol for key exchange suitable for IoT.

Keywords: IoT, postquantum cryptography, information security, postquantum protocols

1 ÚVOD

V posledních desítkách let dochází k radikálnímu technologickému vývoji, který se mimo jiné orientuje i na kvantové počítače. V případě budoucího využití Shorova algoritmu na kvantových počítačích je pravděpodobné, že některé matematické problémy, na které spoléháme, budou vypočitatelné v reálném čase. Kryptografické algoritmy jako například RSA, ECDSA, DSA, které využívají pro svou bezpečnost prvočíselného rozkladu a diskrétního logaritmu, nebudou vůči kvantovým počítačům bezpečné. Z tohoto důvodu se začíná klást důraz na takzvanou postkvantovou kryptografii, která je schopna odolat útokům kvantových počítačů. Kromě běžných stolních počítačů je třeba klást důraz na bezpečnost i v oblasti omezených zařízení. Zařízení SCADA, IoT anebo Průmysl 4.0 jsou projekty, které jsou plánovány výhledově v dlouhodobějším časovém měřítku. Z tohoto důvodu je třeba zahrnout i možnost hrozby ze strany kvantových počítačů. Tato práce se věnuje možnostem omezeného zařízení v postkvantové kryptografii a doporučení vhodného protokolu pro ustanovení klíče z pohledu úrovně bezpečnosti a paměťové a výpočetní náročnosti.

2 POSTKVANTOVÁ KRYPTOGRAFIE PRO OMEZENÁ ZAŘÍZENÍ

National Institue of Standards and Technology (NIST) se rozhodl standardizovat jeden nebo více postkvantových kryptografických algoritmů a vyhlásit tak možnost předkládání návrhů, které se uzavřelo 30. listopadu 2017 [7]. V současnosti se v prvním kole hodnotí přes 50 možných algoritmů. Jen málo z nich se mimo jiné orientuje i na jednodušší zařízení, jako jsou například výpočetně a pamětově omezená zařízení. V této práci testujeme 6 protokolů určených k ustanovení klíče na omezeném zařízení a zjišťujeme, jaká je jejich úroveň bezpečnosti a výpočetní a paměťová náročnost. V práci jsou implementovány a testovány následující protokoly.

- Protokol New Hope je založen na kryptografii mřížek, která využívá matematického problému Ring-LWE, který oproti LWE problému využívá problematiky polynomiálních okruhů nad konečným polem. Jeho úroveň bezpečnosti pro postkvantovou kryptografii je 206 bitů. Bližší informace lze nalézt na [1].
- Protokol BCNS předcházel protokolu New Hope. BCNS je založen na kryptografii mřížek a

Ring-LWE problému. Jeho úroveň bezpečnosti je 76 bitů. Podle požadavků NIST je nedostatečná pro standardizaci. Bližší informace lze nalézt [3] .

- Protokol SIDH vychází z Diffie-Hellmanova návrhu výměny klíčů a vylepšuje ji pro postkvantovou kryptografii. Je založen na supersingulárních eliptických křivkách a jeho úroveň bezpečnosti pro postkvantovou kryptografii 128 bitů. Pro bližší informace se lze podívat zde [5].
- Protokol Frodo je protokol založen na kryptografii mřížek. Oproti ostatním protokolům založených na mřížkách Frodo využívá matematického problému LWE. Jeho úroveň bezpečnosti je 130 bitů. Bližší informace lze nalézt na [4].
- Protokol NTRU je založen na kryptografii mřížek a je založen na matematickém problému Ring-LWE. Jeho úroveň bezpečnosti je 128 bitů. Bližší informace lze nalézt na [6].
- Protokol McBits je založen na teorii kódování a využívá tzv. Goppa kódů. Vychází z protokolu Niederreiter. Jeho úroveň bezpečnosti je 120 bitů. Bližší informace na [2].

3 IMPLEMENTACE NA RASPBERRY PI 3

V rámci této kapitoly jsou otestovány jednotlivé protokoly z hlediska výpočetní a paměťové náročnosti při ustanovení společného klíče. K testování postkvantových kryptografických algoritmů bylo zvoleno výpočetně omezené zařízení Raspberry Pi 3 Model B. Jedná se o jednodeskový mikropočítač s procesorem Broadcom verze armv7l s taktem 1,2 GHz, velikostí operační paměti 1 GB. Uvedený procesor je pouze 32 bitový. Zařízení podporuje řadu operačních systémů, obsahuje bezdrátové rozhraní WiFi 802.11 b/g/n a Bluetooth 4.1. Jako operační systém byl zvolen Raspbian Stretch Lite verze z 29. listopadu 2017, s verzí jádra 4.9. K měření výpočetní a paměťové náročnosti se využily knihovny liboqs verze ze dne 13. ledna 2018 a knihovny OpenSSL 1.0.2n.

Jako první se testovala výpočetní náročnost. Tabulka 1 znázorňuje časovou náročnost jednotlivých kroků při ustanovení klíče mezi stranou Alice a stranou Bob. Jednotlivé sloupce zobrazují časové úseky, které jsou vymezeny buď pro Alici nebo Boba a poslední sloupec znázorňuje celkovou časovou náročnost ustanovení klíče pro daný protokol. Uvedené hodnoty jsou průměrné doby jedné operace z 10-ti měřeních. Z tabulky je zřejmé, že New Hope je nejrychlejší na platformě Raspberry Pi 3. Naopak protokol SIDH vyžaduje jednotky sekund a celková doba je tisícinásobně delší než u protokolu New Hope. Důležité je zmínit, že právě protokol New Hope zajišťuje nejvyšší úroveň bezpečnosti ze všech testovaných protokolů.

Tabulka 1: Časová náročnost postkvantových kryptografických protokolů během výměny klíčů mezi Alicí a Bobem na Raspberry Pi 3.

Protokol	**Alice0** (ms)	**Bob** (ms)	**Alice1** (ms)	**Celkový čas** (ms)
New Hope	0,873 ± 0,002	1,259 ± 0,006	0,226 ± 0,001	2,359 ± 0,007
NTRU	11,215 ± 0,156	0,996 ± 0,015	0,673 ± 0,042	12,884 ± 0,213
BCNS	13,114 ± 0,022	20,222 ± 0,032	1,005 ± 0,002	34,341 ± 0,056
Frodo	350,362 ± 0,031	351,128 ± 0,037	0,631 ± 0,004	702,121 ± 0,072
McBits	1958,941 ± 0,451	0,585 ± 0,003	2,178 ± 0,124	1961,704± 0,578
SIDH	1053,898 ± 1,695	2366,231 ± 3,386	993,874 ±1,411	4414,011 ± 6,484

Dále se testovala paměťová náročnost, která znázorňuje velikost přenesených zpráv mezi Alicí a Bobem před ustanovením společného klíče. Výsledky testování jsou znázorněny v rámci tabulky 2. Z tohoto hlediska byl přenosově nejméně náročný protokol SIDH, který byl naopak časově nejnáročnější. Protokol SIDH byl následován protokolem NTRU a New Hope. Pamětově nejnáročnější je protokol McBits, který k ustanovení klíče využije přes 300 MB.

Tabulka 2: Paměťová náročnost postkvantových protokolů - počet přenesených bajtů při generování klíčů.

Protokoly	**Alice→Bob** (bajt)	**Bob→Alice** (bajt)	**Celkově** (bajt)
SIDH	576	576	1152
NTRU	11027	1022	2049
New Hope	1824	2048	3872
BCNS	4096	4224	8320
Frodo	11280	11288	22568
McBits	311736	141	311877

4 DOPORUČENÍ PRO OMEZENÁ ZAŘÍZENÍ

Obecně lze usoudit, že protokoly založené na mřížkách, které využívají matematického problému Ring-LWE jsou výpočetně méně náročnější než protokoly založené na jiných matematických problémech postkvantové kryptografie. Z hlediska paměťové náročnosti je nejvhodnější protokol SIDH, který je optimalizován tak, aby byl paměťově nejméně náročný. Protokol SIDH je následován protokoly založenými opět na mřížkách a na problému Ring-LWE. Lze tedy obecně říct, že při výběru schématu pro prostředí IoT je vhodné se orientovat na protokoly založené na mřížkách a problému Ring-LWE. Konkrétně práce doporučuje protokol New Hope, který v experimentálním měřením prokázal nejlepší poměr paměťové a výpočetní náročnosti a zaručuje úroveň bezpečnosti 206 bitů.

5 ZÁVĚR

V článku jsou shrnuty výsledky testování postkvantových protokolů pro ustanovení klíče mezi dvěma stranami na omezeném zařízení Raspbery Pi 3 Model B. Důraz je kladen na jejich úroveň bezpečnosti, výpočetní a paměťovou náročnost. Po vyhodnocení výsledků se pro prostředí s omezenými zařízeními jako je IoT jeví jako nejvhodnější kandidát protokol New Hope.

REFERENCE

[1] ALKIM, E. et al. *Post-quantum key exchange – a new hope*. Department of Mathemathics, Ege University, Turkey. [cit. 2017-10-01]. Dostupné z: https://eprint.iacr.org/2015/1092.pdf

[2] BERNSTEIN, J. D et al. *McBits: fast constant-time code-based cryptography*. University of Illinois at Chicago: Department of Computer Science. [cit. 2017-01-20]. Dostupné z: https://www.win.tue.nl/ tchou/papers/mcbits.pdf

[3] BOS, W. J., et al.. *Post-quantum key exchange for the TLS protocol from the ring learning with errors problem*. Microsoft Research, Redmond, Washington, USA. [cit. 2017-12-01]. Dostupné z: https://eprint.iacr.org/2014/599.pdf

[4] BOS, J., et al. *Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE*. ACM CCS. [cit. 2017-11-02]. Dostupné z: https://eprint.iacr.org/2016/659

[5] COSTELLO, C., et al. *Efficient algorithms for supersingular isogeny Diffie-Hellman*. Microsoft Research, USA. [cit. 2017-12-10]. Dostupné z: https://eprint.iacr.org/2016/413.pdf

[6] HOFFSTEIN, J. *NTRU: A Ring-Based Public Key Cryptosystem*. Springer Publishing Company, Incorporated, 2006. ISBN 978-3-540-64657-0.

[7] NIST. *Post-Quantum Cryptography*. National Institute of Standards and Technology. [cit. 2018-02-10]. Dostupné z: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals